Załącznik nr 1 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Wymiana posiadanych przez Zamawiającego urządzeń typu Web Application Firewall firmy Fortinet, na klaster dwóch nowych urządzeń FortiWeb-600F, ze wsparciem technicznym producenta na 3 lata lub równoważnych:

Lp.	Parametr	Wymagania
1.	Architektura systemu	System do ochrony aplikacji webowych, którego zadaniem będzie wykrywanie i blokowanie ataków celujących w witryny i aplikacje webowe oraz informowanie operatora w przypadku wystąpienia określonych zdarzeń. Dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się, aby wszystkie funkcje oraz zastosowane technologie, w tym system operacyjny i sprzęt pochodziły od jednego producenta.
2.	System operacyjny	Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenie musi pracować w oparciu o dedykowany system operacyjny producenta wzmocniony z punktu widzenia bezpieczeństwa.
3	Funkcjonalności	System powinien realizować co najmniej poniższe funkcjonalności: 1. Możliwość zdefiniowania oddzielnych polityk ochrony dla aplikacji webowych umieszczonych na tym samym serwerze Zamawiającego (witryn/virtualhostów znajdujących się pod tym samym adresem IP) 2. Możliwość ochrony danej witryny przed dostępem z puli adresów przypisanych dla danego kraju(ów) 3. Możliwość zablokowania danej witryny przed dostępem z określonych adresów IP 4. Możliwość analizy poszczególnych rodzajów ruchu w oparciu o profile bezpieczeństwa (profil to obiekt określający zbiór ustawień zabezpieczających aplikacje/witryny webowe) 5. Możliwość podziału obciążenia ruchu HTTP na kilka serwerów webowych (loadbalancing) 6. Możliwość skonfigurowania na tym samym adresie IP urządzenia, dostępu do witryn HTTPS posiadających różne certyfikaty SSL (mechanizm SNI) 7. Możliwość skonfigurowania dostępu użytkownika do danej witryny poprzez mechanizm PKI 8. Możliwość przeglądania sesji ustanowionych przez komputery klienckie z uwzględnieniem adresu serwera,

		do którego ruch jest przekazywany. 9. Firewall aplikacji webowych chroniący przed takimi zagrożeniami jak: o SQL Injection o OS Command Injection o Cross Site Scripting (XSS) o Cross Site Request Forgery o Outbound Data Leakage o HTTP Request Smuggling o Buffer Overflow o Encoding Attacks o Cookie Tampering / Poisoning o Session Hijacking o Broken Access Control o Forceful Browsing /Directory Traversal o Inne podatności specyfikowane przez listę OWASP Top 10 10. Firewall aplikacji powinien umożliwiać ochronę przed atakami z udziałem niedopuszczalnych i pustych znaków w adresie URL, przekroczeniach i nieprawidłowościach dla HTTP Request, HTTP Header, HTTP Parameters 11. Możliwość uruchomienia trybu auto-uczenia przyspieszającego i ułatwiającego implementację systemu 12. Możliwość konfigurowania przekierowań - URL rewirting 13. Możliwość ustawienia dostępu do danej części witryny/adresu URL tylko dla określonych adresów IP klientów. 14. Możliwość ochrony witryny przed atakami typu „Brute force” 15. Możliwość ustanowienia polityk ochrony przez atakami typu DoS poprzez ustawienie limitów: HTTP Request Limit/sec, TCP Connection Number Limit 16. Możliwość przekazywania ruchu dla danej witryny internetowej do kilku serwerów www 17. Możliwość dodania nagłówków protokołu http: X-Forwarded-For, X-Real-IP, 18. Możliwość ustanowienia ograniczenia dostępu do danej witryny webowej dla użytkowników serwera LDAP, RADIUS, SAML, OAuth 19. Możliwość ochrony witryny poprzez zastosowanie mechanizmu CAPTCHA 20. Możliwość ustawienia polityki dostępu do danej witryny dla tzw. botów internetowych (Crawlers) oraz

		wyszukiwarek internetowych (Bing – allow, Google – allow, Yandex – deny) 21. Możliwość ustawienia polityki ochrony dla API działającego w formacie JSON oraz XML 22. Możliwość ustawienia mechanizmu przekazywania do analizy przez system Sandbox, pliku załączanego (upload) w witrynie webowej 23. Sprzętowa akceleracja protokołów SSL/TLS zaimplementowanych do ochrony wybranych serwisów webowych
3.	Licencjonowanie	Licencjonowanie bez limitu chronionych serwerów, domen (licencja na urządzenie)
4.	Tryb działania	Możliwość implementacji systemu w trybach Reverse-Proxy lub Transparentnym
5.	Parametry wydajnościowe	Obsługa przepustowości dla ruchu http: 1Gbps lub więcej
6.	Ilość portów sieciowych do obsługi ruchu	1. Nie mniej niż 2 szt. typu 10/100/1000 Mbps Ethernet RJ-45 2. Nie mniej niż 4 szt. typu 1 Gbps Ethernet SFP
7.	Powierzchnia dyskowa	Co najmniej jeden dysk 480 GB SSD
8.	Tryb wysokiej dostępności	W celu zwiększenia niezawodności system powinien mieć możliwość pracy w konfiguracji HA (High Availability) z trybem Active-Passive
9.	Logowanie i raportowanie	1. System powinien umożliwiać lokalne logowanie oraz raportowanie w oparciu o zestaw predefiniowanych wzorców raportów. 2. System powinien mieć możliwość wysyłania logów z urządzenia do serwera typu rsyslog 3. System powinien mieć możliwość wysyłania zdarzeń z urządzenia do systemu typu SIEM
10.	Zarządzanie	1. Interfejs zarządzający dostępny poprzez protokół HTTPS 2. Umożliwienie dostępu do panelu administratora tylko dla zaufanych adresów IP 3. Możliwość wykonania kopii bezpieczeństwa konfiguracji urządzenia na zdalny serwer 4. Śledzenie wykresów z działania systemu w trybie rzeczywistym (np. zajętość pasma dla ruchu http, wykryte zagrożenia, zajętość procesora i pamięci urządzenia)
11.	Montaż i zasilanie	1. Przystosowanie do montażu w szafie teletechnicznej RACK 19” 2. Wysokość pojedynczego urządzenia: maksymalnie 1U 3. Dwa zasilacze na 230V/60Hz

12.	Aktualizacje	Wymagane aktualizacje baz danych sygnatur (w tym antywirusowych), definicji zagrożeń, reputacji adresów IP, lokalizacji GeoIP, przez okres 36 miesięcy od momentu aktywacji wsparcia, aktualizacja sygnatur powinna być wykonywana przez urządzenie automatycznie zgodnie ze zdefiniowanym harmonogramem (min. co cztery godziny)
13.	Gwarancja i serwis	1. Wymagana jest gwarancja i Wsparcie techniczne Producenta przez okres 36 miesięcy od momentu aktywacji u Producenta 2. Zgłoszenia serwisowe mogą być kierowane do producenta w ciągu 24 godzin przez 7 dni w tygodniu 3. Wysyłka nowego urządzenia w następnym dniu roboczym po potwierdzeniu awarii
14.	Integracja ze środowiskiem SOC (Security Operations Center) Zamawiającego	1. Integracja z posiadanym przez Zamawiającego urządzaniem FortiAnalyzer – wysyłanie logów z ruchu oraz wykrytych zagrożeń do urządzenia FortiAnalyzer gdzie dokonywane będzie gromadzenie, przeglądanie i generowanie raportów 2. Integracja z posiadanym przez Zamawiającego urządzeniem FortiSIEM – wysyłanie logów do urządzenia FortiSIEM gdzie dokonywane będzie analiza, wykrywanie i raportowanie zagrożeń 3. Integracja z posiadanym przez Zamawiającego urządzeniem FortiSandbox – możliwość analizy antywirusowej uploadowanych plików do zabezpieczanych przez urządzenie witryn i systemów webowych
15.	Akcesoria dodatkowe	Należy dostarczyć cztery kable, co najmniej 10 metrowe, wraz z czterema wkładkami SFP, umożliwiające podłączenie urządzenia do używanych przez Zamawiającego przełączników sieciowych Cisco 9500-40X
16.	Ilość sztuk	2 sztuki (klaster dwóch urządzeń)

Informacje dodatkowe:

1. Urządzenia będące przedmiotem zamówienia mają zastąpić działające obecnie w infrastrukturze Zamawiającego urządzenia typu WAF firmy Fortinet.
2. Instalacja, konfiguracja nowych urządzeń oraz migracja konfiguracji z dotychczasowych WAF Fortinet Zamawiającego nie jest przedmiotem niniejszego zamówienia.
3. Zamawiający wraz z dostawą nowych urządzeń wymaga dostarczenia nowych licencji oraz kontraktów Wsparcia technicznego Producenta. Nie dopuszcza się przenoszenia doczasowych kontraktów z urządzeń WAF Fortinet Zamawiającego, odnawiania dotychczasowych z przypisaniem do nowych urządzeń, itp.
4. W przypadku zaoferowania rozwiązania równoważnego do produktów firmy Fortinet, Wykonawca zobowiązany będzie do:

a) konfiguracji polityk ochrony na poziomie nie gorszym niż na posiadanych w urządzeniach WAF Fortinet Zamawiającego w terminie, o którym mowa w § 3 ust. 5 Umowy;
b) zintegrowania nowych urządzeń ze środowiskiem SOC (Security Operations Center) Zamawiającego, w zakresie opisanym w tabela 1 pkt 14 w terminie, o którym mowa w § 3 ust. 5 Umowy;
c) zorganizowania co najmniej 3 dniowego szkolenia w trybie on-line, z omówieniem wszystkich funkcjonalności i sposobów zastosowania nowego systemu, dla 3 administratorów, w dniach roboczych w godzinach od 8:00 do 16:00.

5. Wsparcie techniczne Producenta będzie polegało na:
   a) umożliwieniu urządzeniom automatycznego dostępu do usług Producenta, w zakresie opisanym w tabela 1 pkt 12;
   b) umożliwieniu Zamawiającemu pobrania aktualizacji, poprawek bezpieczeństwa i nowych wydań systemu operacyjnego urządzeń, przez 36 miesięcy od dnia aktywacji u Producenta;
   c) konsultacjach poprzez telefon, email lub system zgłoszeniowy web-helpdesk, celem rozwiązania problemów napotkanych podczas eksploatacji urządzenia oraz pomoc w zastosowaniu rozwiązań konfiguracyjnych urządzenia, w czasie 36 miesięcy od dnia aktywacji u Producenta;
   d) zgłoszenia serwisowe mogą być kierowane do producenta w ciągu 24 x 7 dni w tygodniu;
   e) wysyłka nowego urządzenia odbywać się będzie w następnym dniu roboczym po potwierdzeniu awarii urządzenia przez Producenta.

6. Zamawiający wymaga, aby dostarczone urządzenia były fabrycznie nowe. Zamawiający nie dopuszcza składania ofert zawierających sprzęt poserwisowy lub refabrykowany.

7. Wykonawca gwarantuje, iż sprzęt i oprogramowanie dostarczone w ramach realizacji umowy pochodzi z legalnego źródła i nie jest częścią żadnego projektu oferowanego dla innych podmiotów.